2mix

NASA TECHNICAL MEMORANDUM

NASA TM X-64799

(NASA-TM-X-64799) A GUIDE FOR PERFORMING SYSTEM SAFETY ANALYSIS (NASA) ~~45~~ 46 p HC $4.25 CSCL 13L

N74-14689

Unclas
G3/34 26370

A GUIDE FOR PERFORMING SYSTEM SAFETY ANALYSIS

By J. M. Brush, R. W. Douglass III, F. R. Williamson
(Martin C. Dorman, Editor)
Systems/Products Office

January 18, 1974

NASA

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama

TECHNICAL REPORT STANDARD TITLE PAGE

1. REPORT NO. NASA TM X-64799	2. GOVERNMENT ACCESSION NO.	3. RECIPIENT'S CATALOG NO.
4. TITLE AND SUBTITLE A Guide for Performing System Safety Analysis		5. REPORT DATE January 18, 1974
		6. PERFORMING ORGANIZATION CODE
7. AUTHOR(S) J. M. Brush, R. W. Douglass III, F.R. Williamson (Martin C. Dorman, Editor)		8. PERFORMING ORGANIZATION REPORT #
9. PERFORMING ORGANIZATION NAME AND ADDRESS George C. Marshall Space Flight Center Marshall Space Flight Center, AL 35812		10. WORK UNIT NO.
		11. CONTRACT OR GRANT NO.
12. SPONSORING AGENCY NAME AND ADDRESS National Aeronautics and Space Administration Washington, DC 20546		13. TYPE OF REPORT & PERIOD COVERED Technical Memorandum
		14. SPONSORING AGENCY CODE

15. SUPPLEMENTARY NOTES

This document was prepared from technical material developed by personnel of Systems/Products Office, Science and Engineering Directorate, MSFC, and Planning Research Corporation

16. ABSTRACT

This document is a general guide for performing system safety analyses of hardware, software, operations and human elements of an aerospace program. The guide describes a progression of activities that can be effectively applied to identify hazards to personnel and equipment during all periods of system development.

This document describes the general process of performing safety analyses; setting forth in a logical order the information and data requirements, the analytical steps and the results. These analyses are the technical basis of a system safety program. Although the guidance established by this document cannot replace human experience and judgement, it does provide a methodical approach to the identification of hazards and evaluation of risks to the system.

* PRC Systems Services Company

17. KEY WORDS Safety Analysis Systems Safety System Analysis Hazard Analysis	18. DISTRIBUTION STATEMENT Unclassified - Unlimited William H Dodd

19. SECURITY CLASSIF. (of this report)	20. SECURITY CLASSIF. (of this page)	21. NO. OF PAGES	22. PRICE
Unclassified	Unclassified	45	NTIS

MSFC - Form 3292 (Rev December 1972)

For sale by National Technical Information Service, Springfield, Virginia 22151

PREFACE

This document is a general guide for performing system safety analyses of hardware, software, operations and human elements of an aerospace program. The guide describes a progression of activities that can be effectively applied to identify hazards to personnel and equipment during all periods of system development.

This document describes the general process of performing safety analyses; setting forth in a logical order the information and data requirements, the analytical steps and the results. These analyses are the technical basis of a system safety program. Although the guidance established by this document cannot replace human experience and judgement, it does provide a methodical approach to the identification of hazards and evaluation of risks to the system. It draws heavily from and is generally consistent with the requirements of NASA Safety Manual NHB 1700.1, MIL-STD-882, and NASA Safety Program Directive No. 1, Revision A.

Preceding page blank

TABLE OF CONTENTS

Preceding page blank

LIST OF ILLUSTRATIONS

DEFINITIONS

CREW - The term "crew" refers to both ground and flight personnel.

ENERGY RELEASE MECHANISM - Any unsafe condition or act that may couple the energy to a sensitive component, or that could cause unintentional or uncontrolled energy release.

ENERGY NEEDS - Refers to physical energy needs for warning, escape, motion control, information, command, interface capability; and physiological energy needs for human survival and human capability.

ENERGY BLOCKAGE MECHANISM - Means by which the loss of the normal energy supply or excessive energy demands could cause an unsafe (hazardous) condition, or means by which energy supply may be lost or demands may exceed capability.

ENERGY SOURCES - Refers to high energy environments, both natural and induced, such as lightning, wind acceleration, vibration; high energy components, such as pressure vessels, fuels; and low energy phenomena, such as human toxicants, materials deterioration, physical contamination.

FAILURE, PRIMARY - This term refers to failure of a component that was operated in normal sequence within the environmental and time requirements for which it was designed.

FAILURE, SECONDARY - Failure of a component due to out-of-tolerance input from an upstream component or from exposure to an abnormal environment.

FAILURE, SEQUENTIAL - Failure of a component or system due to receiving input signals out-of-sequence.

HAZARD - Any real or potential condition that can cause injury or death to personnel, or damage to or loss of equipment or property. Hazards include: dangerous energy sources and unsafe conditions or unsafe acts that could lead to accidental energy release; lack of needed physical or physiological energy for life support.

HAZARD LEVELS - Hazards are categorized to establish corrective action priorities.

Category I. Catastrophic. The potential hazard could cause death or severe injury to personnel, or significant property loss (more than $100,000) and there is not time for corrective action.

Category II. Critical. The potential hazard could cause personnel injury or major property damage (more than $10,000), and will require immediate corrective action for personnel or system survival.

Category III. Controlled. Caution, warning and protective devices are provided so that the potential hazard can be counteracted or controlled without injury to personnel or major system damage.

Category IV. Negligible. Equipment failures or personnel errors that will not result in personnel injury or major property loss.

PROGRAM/PROJECT HAZARD SUMMARY - A document summarizing identified hazards, corrective action, hazard status and risk acceptance rationale for use in risk management.

RISK - Probability of occurrence of a specific hazard and hazard level.

RISK MANAGEMENT - The process whereby decisions are made to accept a known risk/hazard or to eliminate or minimize the risk/hazard. Trade-offs are made among increased cost, schedule requirements, and effectiveness of redesign, installation of safety or warning devices, and procedural changes to eliminate the risk/hazard.

SAFETY - Freedom from those conditions that can cause injury or death to personnel and/or damage to or loss of equipment or property.

SAFETY GOALS - Reduce severity and probability of occurrence of each identified hazard to an acceptable level (controlled).

SYSTEM SAFETY - The optimum degree of safety within the constraints of operational effectiveness, time and cost, attained through specific application of system safety management and engineering principles throughout all phases of a system's life cycle.

UNDESIRED EVENT - An event which the system being analyzed cannot tolerate, such as a catastrophic loss of that system's equipment or loss of the crew.

PART 1: MANAGEMENT PERSPECTIVE

A. INTRODUCTION

The project manager must plan a safety program that will include the identification and elimination or control of hazards in ground and flight equipment and operations. In a few instances, certain known risks may have to be taken. The acceptance of these risks or residual hazards, should be based on thorough visibility as to the nature of the hazards and risks and of the options and alternatives to their acceptance.

B. PURPOSE AND SCOPE

This section summarizes for the project manager those preliminary and subsequent safety activities that must be accomplished in order to:

1. Identify hazards in the system
2. Determine corrective actions that may be implemented to either eliminate or control the hazard.
3. Decide whether to accept a risk. This activity requires that the System Safety Analyst integrate the findings of safety analyses with those of other engineering analyses such as sneak circuit analyses, thermal analyses, stress analyses, etc., which indicate system hazards, into Risk Management.

The project manager will consider available funds, his need for systems safety visibility, and criticality of the mission prior to deciding upon the required level of safety analysis effort.

C. ORGANIZATION

As a general rule, to maintain objectivity and a check and balance system, it is preferable that system safety not be part of nor subordinate to the design engineering organization. System safety should, however, be an active participant in design and development activities. Regardless of organizational structure, system safety analyses must be performed by personnel who have an intimate knowledge of the system, crew interfaces and mission operations.

D. PRELIMINARY SAFETY ACTIVITIES

Planning for the safety effort will include a Functional Hazard Analysis and related tasks. These tasks, which become the foundation for system safety efforts during system definition, design, manufacture, test and operation, are:

1. Review of pertinent historical safety data from similar systems.
2. Development of safety guidelines and constraints based on mission objectives and experience from previous programs. These will guide the considerations of various concepts for meeting the objectives.
3. Continuing review of the gross hardware requirements, concepts and documentation as the program/project develops.
4. Review of the proposed mission objectives for safety considerations.
5. Performance of a functional hazard analysis to identify potentially hazardous functions and system elements, undesired events, and to develop initial safety requirements and criteria.
6. Performance of trade studies with the result of the functional hazard analysis identifying highly hazardous areas, with recommendations for elimination or control of the hazard or of possible alternatives.
7. Identification of requirements for special safety studies. These should normally be required during system definition or preliminary design in order to be cost effective.
8. Estimation of resource requirements for system safety analysis during the complete system life cycle.
9. Establishment of a system for retaining the following safety data developed during the program life cycle: results of analysis, safety criteria and requirements, results of special studies and applicable historical data, risk decisions and rationale.
10. Establishment of a system safety output schedule to coincide with major program/project milestones to assure timely and effective application of safety principles in the solution

of major problems.

E. SUBSEQUENT SAFETY ACTIVITIES

Detailed safety analyses are conducted by formalized techniques which are identified as Fault Hazard Analysis, Procedures Analysis, and Human Factors Analysis. These analysis techniques, described in Part II of this guide, are intended to provide systematic determination of:

1. Undesired events
2. Safety criteria and requirements
3. Extent to which safety criteria and requirements have been included in the design
4. Whether safety criteria and requirements created for a specific design have provided adequate safety for the system
5. Means for meeting pre-established safety goals
6. Means for demonstrating that safety goals have been met
7. Factors that may cause secondary component failures
8. Factors that may cause sequential failures
9. Need for further analyses
10. Critical fault paths
11. Critical components
12. Procedural discrepancies
13. Corrective action to reduce hazards
14. Factors contributing to hazardous human errors
15. Hazardous failure occurrence
16. Potential effect of hazard upon crew

F. RISK MANAGEMENT RELATIONS

The process of risk management involves the evaluation of hazards identified by the safety analyses to determine appropriate actions required: To control the hazard or to accept the risk involved. The control may consist of such actions as a design change, addition of safety devices, development of caution and warning capabilities, or changes in procedures. Acceptance of risk is a decision in which impacts on cost, schedule, or performance outweigh the risk of occurrence of the hazard.

Risk management iterates as the program matures and as the requirements/specifications develop in depth and coverage. The iterative process and the need for data recall require that the decisions made within the responsibilities of risk management be completely documented together with the analytical data, safety requirements generation, decision rationale, impact versus risk evaluations and directed corrective action. These data comprise the Program Hazard Summary.

Figure 1 depicts and summarizes the risk management concept and the Program Hazard Summary relations.

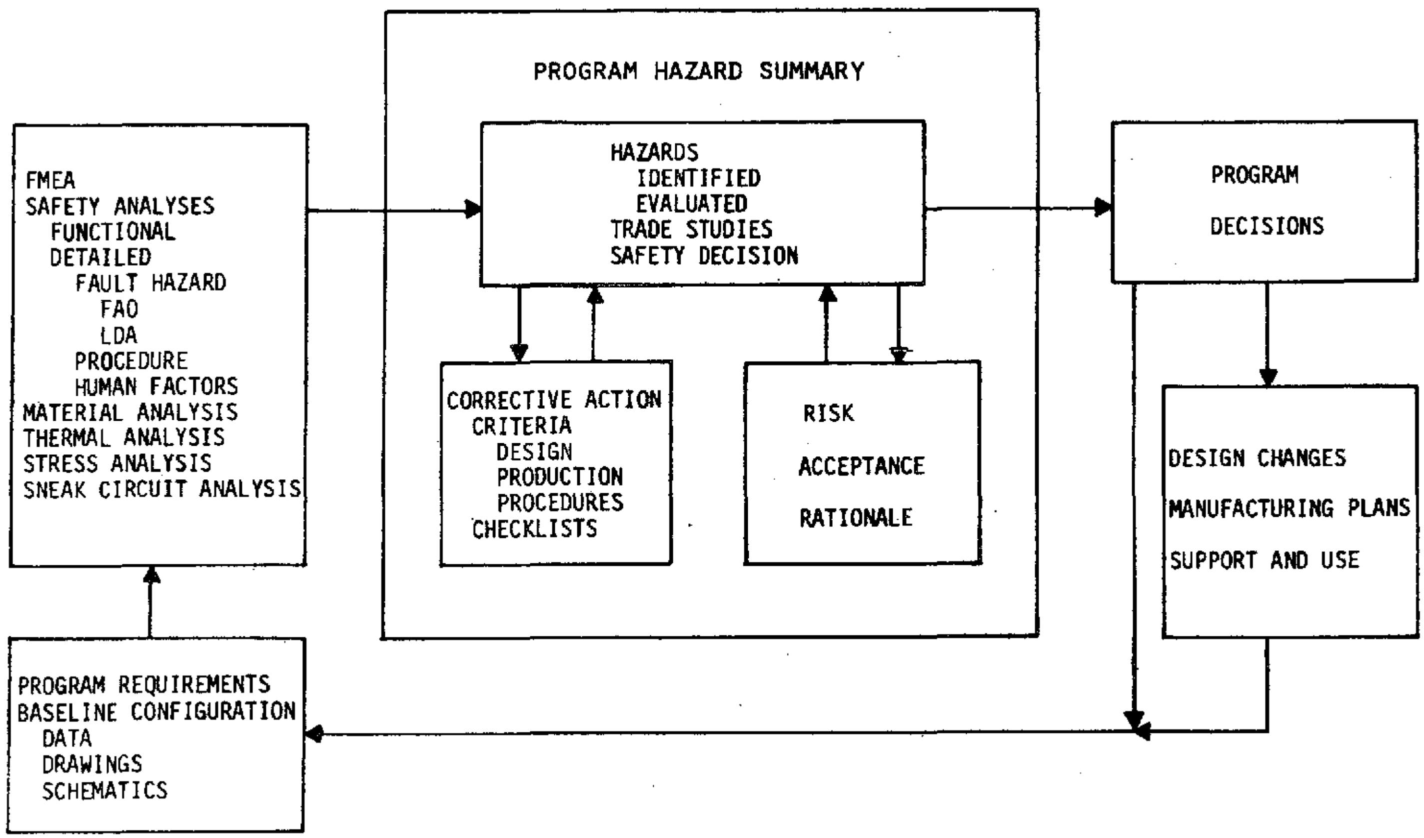


FIGURE 1. RISK MANAGEMENT RELATIONS

PART II: TECHNICAL METHODS

A. INTRODUCTION

The formalization of the system safety analyses in the development programs of MSFC requires technical methods that are generally accepted as tools of the system safety technology. Data utilized as a basis for conducting these analyses consists of specifications, system descriptions, flow diagrams, engineering drawings and related data. Section C summarizes four of these methods: Sections D, E, F, and G describe them.

B. PURPOSE AND SCOPE

1. Part II describes in broad terms the technical system safety methods that are available for accomplishing risk evaluation. This evaluation will serve as a basis for a decision to accept the risk or require a design concept, design or procedural change. The evaluation methods are described in sufficient detail to provide an understanding of the techniques and permit an evaluation of the analysis results. For additional information refer to systems safety and hazard analysis publications listed in Appendix A.

2. The methods described herein are applicable to all MSFC systems. The analysis methods may be expanded, reduced or altered as required to suit the specific needs of any project, thus assuring maximum flexibility.

3. The major reasons for undertaking system safety analyses are to:

   a. Identify hazards in a system so they can be eliminated, controlled or minimized

   b. Categorize the hazards in terms of

      (1) Relative severity of the hazard, which is the effect on the system should the hazardous event occur.

(2) Mission phase during which the hazardous event can affect the system.

(3) Likelihood of hazardous event occurrence.

c. Develop recommendations for corrective actions.

d. Evaluate corrective action taken by a designer to eliminate or control identified hazards.

e. Systematically search for alternatives to acceptance of risks during testing or operation of the system.

f. Develop a continuing Project Hazard Summary utilizing all sources of information pertinent to the life cycle of the system. These sources will include system analyses, sneak circuit analysis thermal analyses, stress analyses and other engineering analyses which will aid in identifying system hazards. This summary identifies the hazard, and control action, residual hazard, and risk acceptance for Risk Management. (See Section F of Part I.)

C. TECHNIQUES FOR SYSTEM SAFETY ANALYSIS

Four system safety analytical methods, see Figure 2, are described in their logical order of progression. The amount of progression, and extent and depth of analytical coverage is determined by project management based on its need for safety visibility.

1. Functional Hazard Analysis

This analysis identifies hazards associated with major mission events and energy sources. It is a non-detailed preliminary analysis usually associated with the early phases of a project. This analysis identifies gross areas of concern in mission and system concepts, and recommends specific areas for further analysis in subsequent safety activity. An activity associated with Functional Hazard Analysis is the identification or development of system safety requirements and review of requirements and safety standards for applicability with respect to project characteristics. See Section D for description.

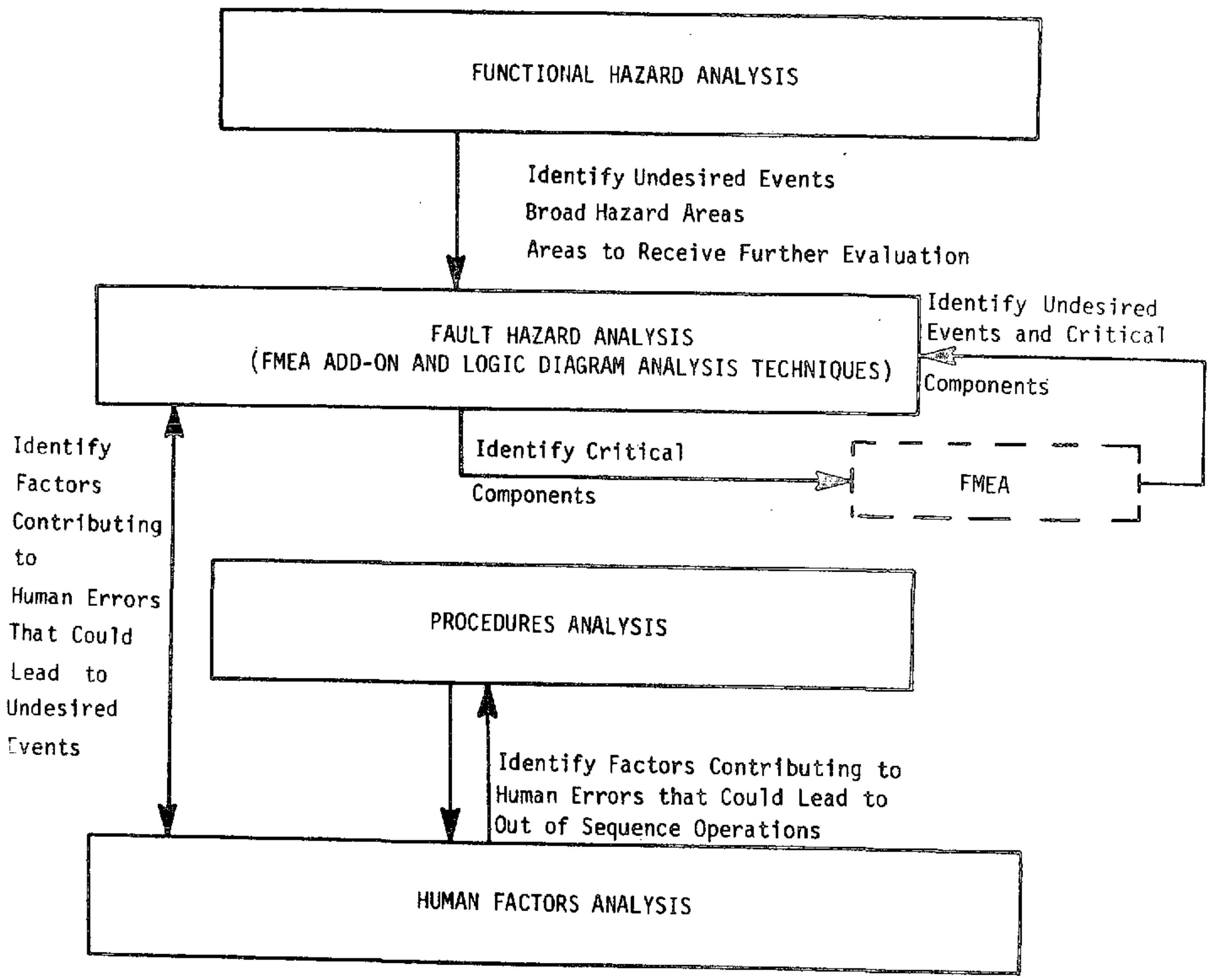


FIGURE 2. SYSTEM SAFETY ANALYSIS METHODS AND RELATIONSHIPS

2. Fault Hazard Analysis

As the system becomes better defined and more detailed design data evolve, Fault Hazard Analysis can be undertaken. This analysis can be accomplished by the Failure Mode and Effect Analysis (FMEA) Add-On or the Logic Diagram Analysis (LDA) technique. See Section E for description.

3. Procedures Analysis

Manufacturing, testing, checkout, training and operating procedures should be analyzed to assure safety of the system and of the human operators. See Section F for a further discussion.

4. Human Factors Analysis

Human Factors considerations are an adjunct to the foregoing analyses to assure incorporation of the Human Element in evaluations. Human Factor considerations will be incorporated into Fault Hazard Analyses concurrent with the system concept and shall be refined as Ground/Flight crew responsibilities and procedures become definitive with respect to test, operations, maintenance,etc. See Section G for a further discussion.

D. FUNCTIONAL HAZARD ANALYSIS

1. General

a. The purpose of the Functional Hazard Analysis, the first analysis in the progression, is to identify safety critical areas and hazards to be resolved during feasibility studies or system definition activities. This analysis provides a comprehensive identification of hazards commensurate with generic system definition and is accomplished as early in the program as possible.

b. Information required to do this analysis falls in two categories:

(1) safety data (e.g., checklists, design guides, general failure data) from previous pertinent programs

(2) system and subsystem descriptions of systems being analyzed.

c. A portion of the Human Factors Analysis (see Section G) will be done as a step in the Functional Hazard Analysis where consideration is given to factors which could induce human errors that might cause undesired events. The results of the Functional Hazard Analysis will be used as a starting point for Fault Hazard, Procedures and Human Factors Analyses.

2. Method of Analysis

a. The Functional Hazard Analysis will:

(1) Review pertinent NASA experience and data produced by other agencies to take advantage of previous similar safety experience. This safety data, e.g., standard checklists, design guides, and failure experience will be tailored to more nearly match the mission and system characteristics of interest.

(2) Review System Design data related to the evolving system.

(3) Identify all energy sources and energy needs such as:

(a) High Energy Environment

(b) High Energy Components

(c) Low Energy Phenomena

(d) Physical Energy Needs

(e) Physiological Energy needs

(4) Identify design features or procedures that have been developed to control energy release mechanism or energy blockage mechanism.

(5) Identify energy release mechanism or energy blockage mechanism for which inadequate controls have been adopted.

(6) Identify safety requirements and criteria incorporated or needed to assure control of the energy release mechanism or energy blockage mechanisms.

(7) Reiterate the process in those areas where major program changes occur.

(8) Use results of the analysis as applicable for an input to trade studies and reviews.

b. In performing a Functional Hazard Analysis the analyst will prepare a chronological listing of functions or events. He will then relate these functions and events to the systems operating during these events. An example listing of mission functions or events with functional systems to perform those functions on manned space vehicles is presented in Figure 3.

c. The next step in the Functional Hazard Analysis is to identify energy sources/needs and related hazards which are applicable to each of the defined functional systems. The energy source/need and hazard identifications are largely based on data and experience from previous programs and/or system functional diagrams. Figure 4 presents hazards for only one of the mission events. It shows undesired events and their causes for the functional systems defined for a launch-boost phase. Safety features and evaluation for adequacy of control of the hazardous events are then reviewed to identify areas needing further consideration.

d. A further step in the Functional Hazard Analysis is to consider factors which could induce human errors that might cause undesired events. For information on human error analysis (e.g., factors and limits) see Section G.

3. Results

This analysis will give the preliminary identification of the following items, which can be presented in Figure 4 format:

MISSION EVENTS	FUNCTIONAL SYSTEMS
PRE-LAUNCH	Engines, Flight Control, Fuel, Oxidizer, Staging, Guidance, Electrical, Propellant Dispersion, Telemetry, Launch Escape System, Structures
LAUNCH-BOOST	Engines, Flight Control, Fuel, Oxidizer, Staging, Guidance, Electrical, Propellant Dispersion, Telemetry, Launch Escape System, Structures
FAIRING SEPARATION	Separation, Electrical, Structures, Ordnance
ORBITAL INJECTION	Engine Shutdown, Payload Separation, Electrical, Guidance, Structures, Mechanical
SOLAR PANEL DEPLOYMENT	Squib, Unfolding, Electrical, Navigation, Structures
ATTITUDE POSITIONING	Reaction Control, Electrical, Navigation, Mechanical
ORBIT CORRECTION	Propulsion, Computer, Electrical, Navigation
DATA ACQUISITION	Antenna, Telemetry, Computer, Electrical
MID-COURSE CORRECTION	Propulsion, Computer, Navigation, Electrical
STAR ACQUISITION	Navigation, Reaction Control, Computer, Electrical
DATA ACQUISITION AND TRANSMISSION	Sensing, Data Storage, Telemetry, Electrical

FIGURE 3. TYPICAL MANNED MISSION EVENTS AND FUNCTIONAL SYSTEMS

PROJECT ____________ FUNCTIONAL HAZARD ANALYSIS SHEET NO. ___ of ___

MISSION EVENT LAUNCH - BOOST DATE ____________

FUNCTIONAL SYSTEM	ENERGY SOURCE/NEED	HAZARD	UNDESIRED EVENTS	HAZARD CATEGORY	RECOMMENDED SAFETY ACTION	REMARKS
ENGINES	High pressure lines, valves, thrust chamber	Loss of one engine thrust, engine explosion	Loss of total stage thrust - vehicle loss			
FLIGHT CONTROL	High pressure pump, valves & lines	Hydraulic actuator leak or seizure, erroneous signal.	Loss of thrust vectoring - vehicle loss			
FUEL	High pressure lines	Pressure switch fails to actuate, fuel leak	Engine shutdown vehicle loss			
OXIDIZER	High pressure lines	Lox leak	Engine shutdown			
STAGING (Rocket)	Solid fuel	Motor case rupture	Loss of staging-vehicle loss			
GUIDANCE	Guidance signal need	Receiver or transmitter malfunction	Loss of flight control, guidance vehicle loss			
ELECTRICAL	Voltage and current source or need	Open circuit, short circuit source, or control malfunction	Loss of flight control, guidance vehicle loss			
PROPELLANT DISPERSION	Ordnance	Inadvertent actuation	Loss of thrust-vehicle loss			
TELEMETRY	Signal need	Sensor malfunction	Loss of parameter monitoring-degradation			
	Power/signal need	Transmitter malfunction	Loss of space vehicle status monitoring-loss of mission			

FIGURE 4. FUNCTIONAL HAZARD ANALYSIS

a. Functional System

The systems required to perform the functions necessary to meet the program objectives are called functional systems and will contain hazardous elements, such as; energy sources or energy needs.

b. Energy Source/Need

An energy source (such as; pressurized tanks or lines) is a hazardous element from which uncontrolled energy release could cause personnel injury or equipment damage. An energy need is a hazardous element necessary for safe completion of a mission; such as; emergency signal generator or oxygen for life support.

c. Hazard

The energy release mechanism (such as; high pressure lox leak or motor case rupture) which would cause an uncontrolled energy release is one class of hazard. Another class is the energy need blockage mechanism, such as; signal relay failure or life support oxygen control valve failure.

d. Undesired Event

If a hazard occurs, the result could be one or more undesired events, such as; loss of stage thrust, loss of vehicle or loss of oxygen.

e. Hazard Category

These categories are defined on page v above.

f. Recommended Safety Action

Recommendations and comments are developed to identify proposed actions to eliminate or control the identified hazards.

g. Remarks

Comments are included to identify the need for residual hazard evaluations.

The results of the Functional Hazard Analysis are compiled for inclusion in the Program/Project Hazard Summary.

E. FAULT HAZARD ANALYSIS

1. General

a. The purpose of the Fault Hazard Analysis (FHA), the second analysis in the progression, after further system definition, is to identify component conditions, human factors and procedural discrepancies which could lead to undesired events. These identified components should be the first ones analyzed by Failure Mode and Effect Analysis (FMEA). In the event that FMEA's are completed first, the results of the FMEA analysis will be used as input to Fault Hazard Analysis. The Fault Hazard Analysis and FMEA can, however, be conducted independently of each other.

b. Fault Hazard Analysis, accomplished by means of the FMEA Add-On (FAO) and Logic Diagram Analysis (LDA) techniques, is explained in paragraphs 2a and 2b. The systems analyst must have the same information and knowledge to perform an FHA by the FAO as by the LDA technique. The primary difference is in the starting point and in the method of presenting the final results. The FAO starts with each component to be analyzed and considers upstream and other component failures and human factors which could affect the subject component. The LDA starts with the "undesired event" and works back toward possible causes. The final result of the FAO is a table of component failure causes which supplements the FMEA whereas the final result of the LDA is a series of logic diagrams showing undesired events and possible human factor, procedural discrepancies and component failure causes of the undesired events. (See Figure 5).

c. Types of information used in performing Fault Hazard Analysis are:

(1) Functional Hazard Analysis results.
(2) System requirements
(3) Drawings
(4) Specifications
(5) Hardware system descriptions
(6) Mission time lines
(7) Historical data on similar systems and components
(8) Test data
(9) FMEA's

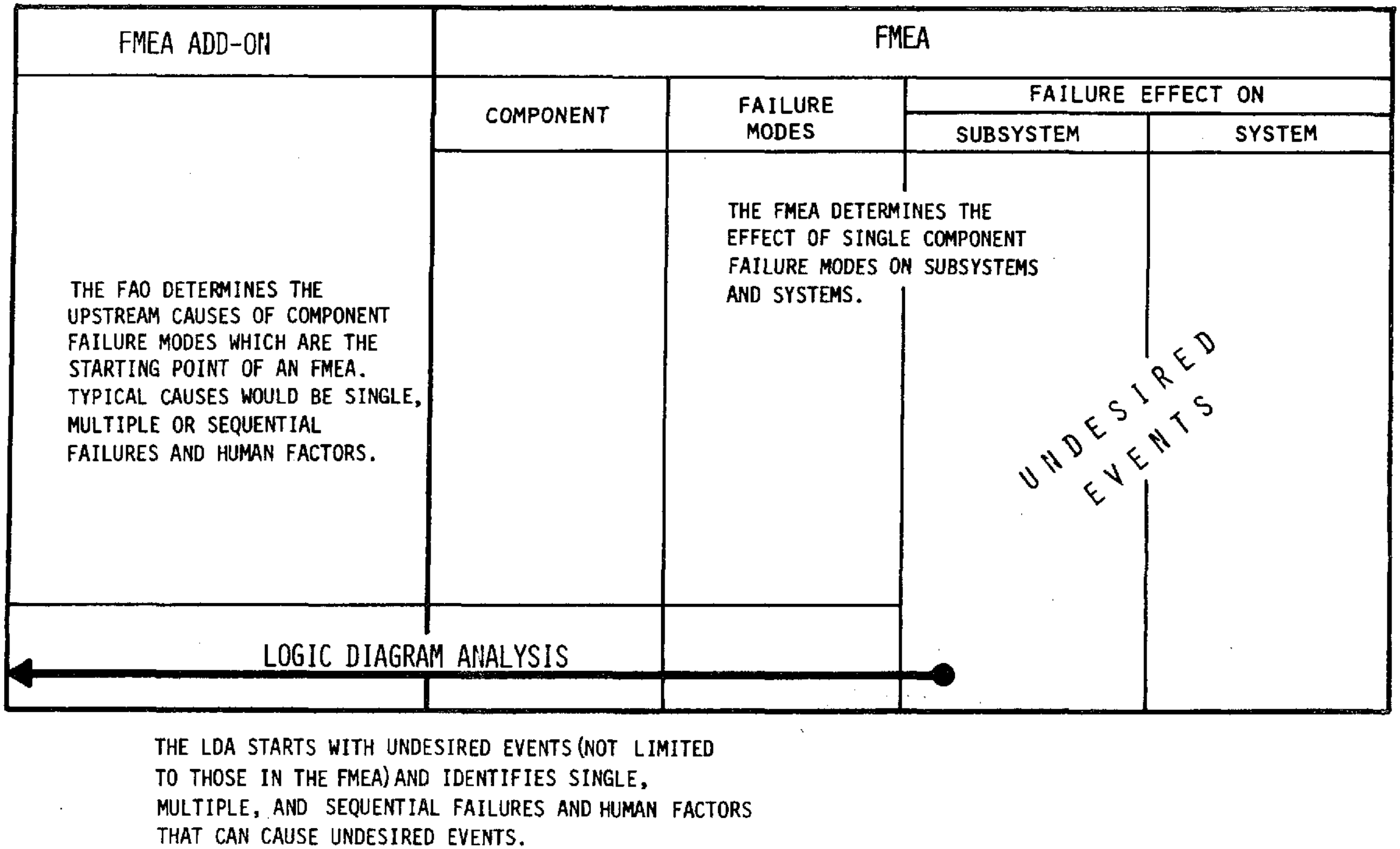


FIGURE 5. FMEA ADD-ON, FMEA, LDA RELATIONSHIP

d. Logic Diagram Analysis starts with undesired events identified in the Functional Hazard Analysis and FMEA. Human factors discussed in Section G must be considered when determining possible causes which lead to undesired events.

2. Methods

a. FMEA Add-On Technique

This technique builds on the FMEA through further system engineering analyses. (See format in Figure 6).

(1) An analysis is made to determine what combination of failure conditions existing simultaneously could result in an undesired event. An example of this type of occurrence would be, as shown in Figure 7, "power remains on pressure switch contacts when switch fails closed "and" pressure switch contacts fail to open after tank presurized." This combination of failures would result in "relay not de-energized after tank pressurized". This information would be listed in column (2) of Figure 6.

(2) An analysis is made to identify conditions which could lead to human errors that might result in an undesired event. The conditions identified might directly effect the component being analyzed or may effect the sequence, duration, or magnitude of upstream input signals or loads to the component being analyzed. If the condition affects the component directly, the conditions will be described in column 3; if the effect results in secondary or sequential failure of the component this information will be entered in column 4 or 5 as appropriate.

(3) A determination is made regarding which failures upstream from each component being analyzed could result in an undesired event. An example would be a fluid or gas pressure above or below that for which the component was designed to operate. An abnormally high pressure could result in secondary structural failure of the component being analyzed, whereas too low a pressure could result in failure of the system to operate properly. Upstream failures that can cause out-of-tolerance conditions effecting components being analyzed should be listed in column 4 of Figure 6.

FMEA ADD-ON TECHNIQUE					
Component Identification 1	Multiple Failures That May Cause Component Failure 2	Human Factors That May Cause Component Failure 3	Factors That May Cause Component Secondary Failure 4	Factors That May Cause Component Sequential Failure 5	Remarks 6

FIGURE 6. FAULT HAZARD ANALYSIS, FMEA ADD-ON

(4) An additional analysis is made regarding the possible ways in which failures of upstream components could result in an operational sequence failure due to premature or delayed input signals to the component being analyzed. Sequentially improper outputs of upstream components should be identified and listed in column 5 of Figure 6. These upstream component failures are responsible for "premature" or delayed" operation failure modes for components analyzed in the FMEA.

b. <u>Logic Diagram Analysis Technique</u>

A sample logic diagram, Figure 7, is a top-down graphic representation of the various parallel and series combinations of subsystem failures which can result in an undesired event. The accomplishment of a Logic Diagram Analysis is undertaken in the following series of steps:

(1) Identify undesired events from Functional Hazard Analysis or checklists from other programs.

(2) Develop the logic diagram by determining the parallel and series events which may cause the undesired events to occur. This process is continued through the appropriate system, subsystem, component, or piece-part level in order to satisfy the scope of analysis previously approved. The series and parallel events are connected by use of graphic symbols. The process of constructing a logic diagram is described in NASA Safety Manual NHB 1700.1 (V3), Boeing Document D2-113072-2 Fault Tree Analysis and Electronic Industries Association Safety Engineering Bulletin No. 3.

(3) Identify critical fault paths (those chains of events which are the most likely to result in a particular undesired event or potential accident). There may be several chains of various degrees of dominance. These chains and their associated degrees of dominance are most clearly identified in the system safety model (logic diagram). The system safety analyst will determine critical fault path(s) and their relative degree of dominance.

(4) Concentrate the initial corrective action on the most critical fault path since this is the most likely avenue along which the undesired event can occur. It may be necessary, however, to consider other paths within the model for the occurrence of a particular undesired event or potential accident.

SEE FIGURE 8 FOR EXPLANATION OF SYMBOLS

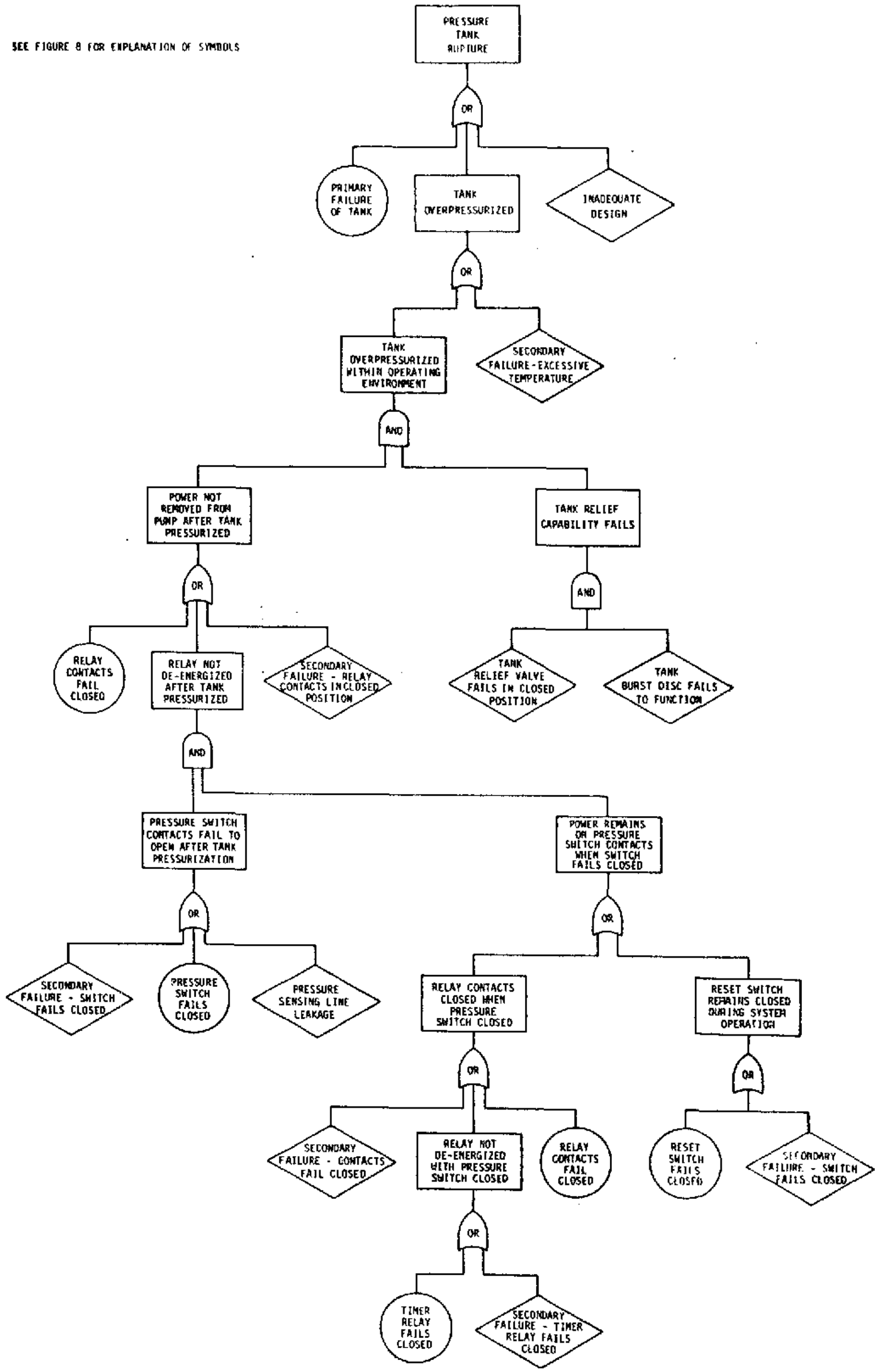
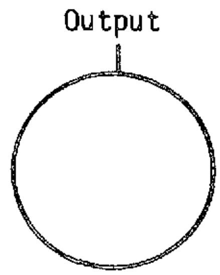
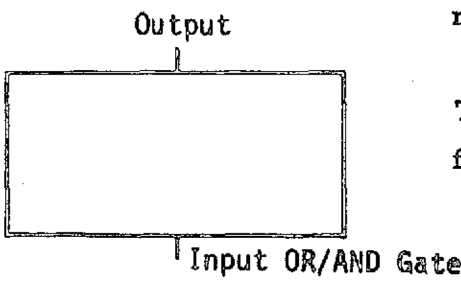


FIGURE 7. LOGIC FOR PRESSURE TANK RUPTURE

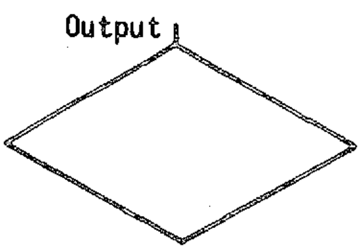


The CIRCLE identifies a component PRIMARY FAILURE.

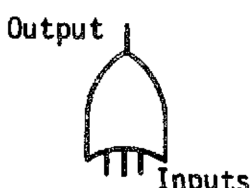
The component failed in spite of being properly designed and operated within the design requirements for environment and electrical, hydraulic, mechanical or other input. This may be a component which had a manufacturing defect that was not detected by quality control or test verification.



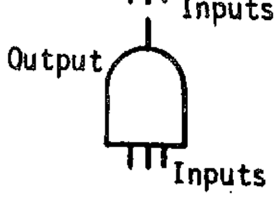
The RECTANGLE identifies an EVENT that results from a combination of fault events.



The DIAMOND identifies a failure which has not been fully developed due to lack of sufficient information.



The OR GATE describes the logical operation whereby the output is caused by the occurrence of any of the inputs.



The AND GATE describes the logical operation which requires the coexistence of all inputs to cause the output.

FIGURE 8. LOGIC DIAGRAM SYMBOLS

(5) Assure that the system safety model (logic diagram) for a given undesired event or potential accident has been developed to the extent necessary to identify critical fault paths. As a minimum the logic diagram development must consider all the safety features and devices which have been designed into the system. This assures that adequate consideration has been given to those areas of the system which contain the greatest identified risk. Safety features and devices are normally placed where there exists the greatest risk of undesired event occurrence.

(6) Determine by logical inspection, the degree of dominance for those critical fault paths of the model which contribute the most to the risk. Logical inspection is the logical thought process of a trained and experienced analyst being applied through examination of the model. This process, associated with whatever experience factors he may consider during the examination to determine which events "look to be" more probable than others, would lead to the resulting statement by the analyst: "these events (identified) and critical fault path(s) look to be the most probable." (See Figure 9). Since the purpose of the evaluation of a diagram is to evaluate the critical fault paths and establish their relative significance, the diagram must be simplified by inspection to minimize the logic diagram structure to be evaluated. This inspection results in elimination of those events and branches which are obviously insignificant compared to others.

c. <u>Comparison of the Logic Diagram Analysis with the FMEA</u>

The Logic Diagram Analysis considers single and multiple failures (occurring simultaneously or in sequence) and human errors. This analysis considers failures that will lead to equipment and/or crew loss. The FMEA generally considers single failure points that lead to crew, equipment, and/or mission loss; it does not consider human errors or multiple failures. MSFC document 85M03885 presents a typical detailed discussion of how to perform a Failure Mode, Effect and Criticality Analysis. See Figure 10 for a comparison of FMEA and Fault Hazard Analysis conducted by LDA.

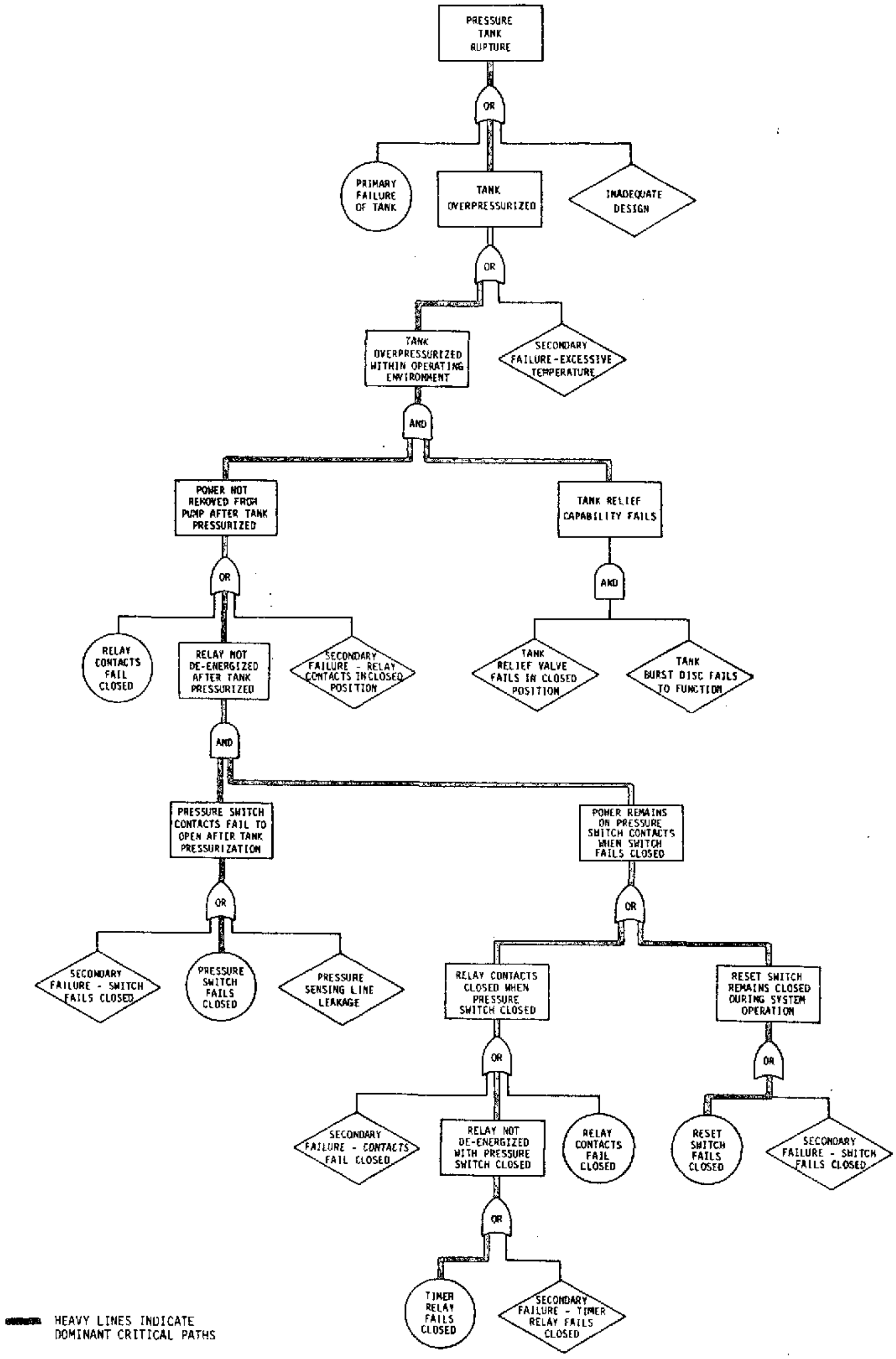


FIGURE 9. LOGIC DIAGRAM DOMINANT CRITICAL PATHS

Analysis Technique \ Failure, Loss, Error	Single Failure Points	Multiple Failures	Sequential Failures	Human Errors	Mission Loss	Crew Injury Or Loss	Equipment Loss
FAULT HAZARD ANALYSIS (FHA)	X	X	X	X		X	* X
FAILURE MODE & EFFECT ANALYSIS (FMEA)	X		X		X	X	X

*Equipment loss that results in crew injury or death

FIGURE 10 FMEA AND FHA COMPARISON

Figure 11 represents the relationship between the LDA and the FMEA. Either the LDA or the FMEA could be the first analysis prepared. In the case where the LDA is the first analysis prepared, certain components (A and B on figure 11) are identified whose failure could lead to an undesired event. These same components should be analyzed further during the preparation of the FMEA. If the FMEA is prepared first, the undesired events identified in the FMEA ("Failure Effect on" section in Figure 11) are then analyzed by the LDA to determine if human errors or multiple failures (not considered by the FMEA) could produce the same undesired event.

3. Results

The Fault Hazard Analysis will identify the following causes of undesired events:

a. Component or part failures

b. Secondary failures

c. Sequential Failures

d. Multiple failures

e Inadequate safety features

F. PROCEDURES ANALYSIS

1. General

a. The purpose of Procedures Analysis, third analysis in the progression, is to define and recommend incorporation of safety requirements that should be met to assure safety of the system, ground crew and flight crew during system operation.

b. Data required for the performance of this analysis include:

(1) Drawings, specifications and hardware (system) descriptions

(2) Test and operational procedures

(3) Manufacturing processes

(4) Mission time lines or test requirements

(5) Results of all safety analyses previously performed

(Cont'd on page 31)

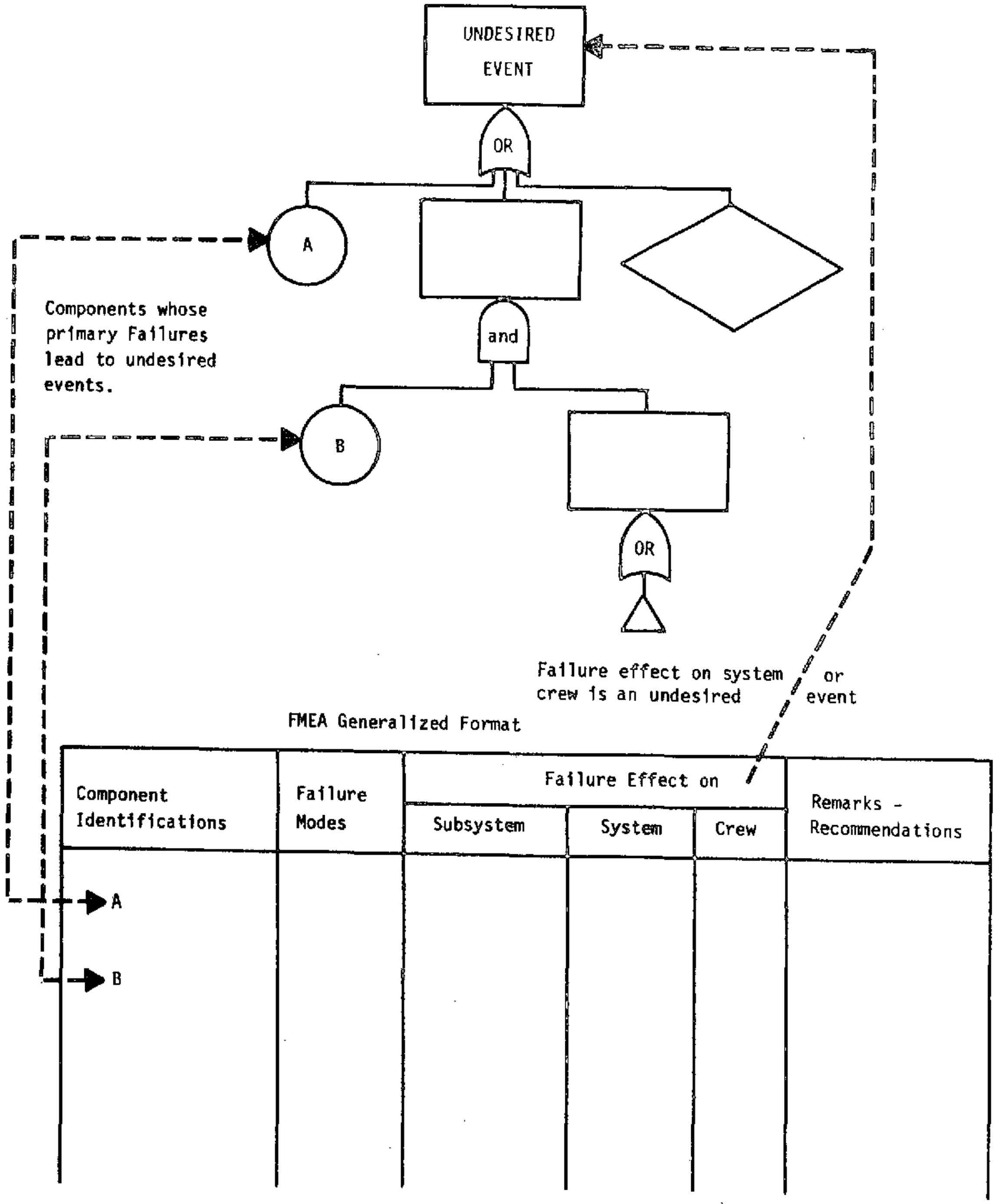


FIGURE 11. RELATIONSHIP OF LDA TO FMEA

END ITEM ______ SUBSYSTEM ______ FUNCTIONAL ASSEMBLY ______			FAILURE MODE AND EFFECTS ANALYSIS							PAGE ______ OF ______ DATE ______ BY ______			
					FAILURE EFFECT ON							
ITEM IDENTIFICATION (1)	FUNCTION (2)	FAILURE MODE (3)	FAILURE REACTION TIME (4)	MISSION OR OPERATIONAL PHASE (5)	FUNCTIONAL ASSEMBLY OR SUBSYSTEM (6)	END ITEM OR OTHER SYSTEMS (7)	MISSION (8)	CREW OR VEHICLE (9)	FAILURE DETECTION METHOD (10)	CORRECTIVE ACTION (11)	CRITICALITY CATEGORY (12)	REMARKS (13)

FIGURE 12. TYPICAL FMEA FORMAT

Column Number	Entry Description and Explanation
1	Name of the element or component under analysis, and reference designation used to identify the element on the schematic. Also, drawing number by which the contractor identifies and describes each item, and coding designation used to identify the item on the block diagrams.
2	Concise statement of the function performed.
3	Enter and describe the specific failure mode after considering the four basic failure conditions: Premature operation Failure to operate at a prescribed time Failure to cease operating at a prescribed time Failure during operation
4.	Estimate of time from failure occurrence to ultimate failure effect.
5.	Operational or mission phase in which the critical failure occurs. For lower level FMEA's where the mission phase such as boost, orbit, etc. is unknown, the system's operational modes should be substituted.
6, 7	A brief description of the effect of the failure on the functional assembly of which the item being analyzed is a part and next higher assemblies. For analysis purposes, the effects of a failure on the next higher assemblies shall be classified as follows:

FIGURE 12. (EXPLANATION)

Column Number	Entry Description and Explanation	
	Effect	**Probability of Occurrence P(x)**
	Actual Loss	$P(x) = 1.00$
	Probable Loss	$0.10 < P(x) < 1.00$
	Possible Loss	$0 < P(x) \leq 0.10$
	No effect	$P(x) = 0$
8.	Describe the effect of the failure on the mission or operational objective of the end item. See (6,7) above for effect categories.	
9.	A description of the effect of the failure on crew or vehicle safety or both. See (6,7) above for effect classifications.	
10.	A description of the methods by which the failure is detected. If not readily detectable, indicate how testing or adding of test points would lead to detection.	
11.	A description of the recommended corrective actions that the using personnel or the maintenance crew could take to circumvent (work around) the failure.	
12.	State the criticality category.	
13.	List any pertinent information not included in the other columns.	

FIGURE 12. (EXPLANATION)

(6) Historical data from previously performed tests and operations of similar systems.

c. Undesired events and hazardous conditions and elements identified in the Functional Hazard and Fault Hazard Analyses will be used as a basis for determining if any procedures or combinations of procedures could lead to identified hazards. Consideration of the potential for human error will be an inherent part of this analysis. Factors described in Section G will serve as guidelines for assessing the potential for human error in the procedure analysis.

2. Method of Analysis

a. This analysis technique involves a review of all requirements, procedures, and actual practices associated with the program. Emphasis is placed on completeness of procedures, including all cautions to be exercised regarding inadvertent out-of-sequence operations, and inclusion in the procedures of adequate recycle and backout instructions to counter potential emergency situations.

b. The procedures safety analysis is performed in three steps as follows:

(1) Review test or operations requirements documentation and develop or review safety requirements appropriate to procedures and recommend inclusion of these requirements into the document.

(2) Review the manufacturing, packaging, handling, storage, transportation, maintenance, test, operation and emergency procedures to verify that the safety requirements included in the requirements documentation have been included in the procedures. Special attention should be devoted to backout and shutdown capability. Manufacturing procedures are to be examined to assure that no process will subsequently result in a hazardous condition for the system or its flight crew.

(3) Review developmental, qualification, acceptance, and system validation testing procedures. Also review test procedures and actual testing during pre-launch checkout. Reiterate the procedures safety analysis for any major design and procedural changes.

3. <u>Results</u>

a. Identification of corrective action necessary for avoiding or reducing hazards and development of justification for these actions. Possible corrective actions:

(1) Procedural controls to be imposed

(2) Warning and caution notes to be inserted in operation and maintenance procedures

(3) Emergency procedures to be developed

(4) Testing safety requirements to be specified

(5) Requirements for emergency equipment and its location to be developed

(6) Safety restrictions and regulations to be implemented

(7) Safety training requirements to be implemented

G. HUMAN FACTORS ANALYSIS

1. <u>General</u>

a. The purpose of the Human Factors Analysis, the fourth in the progression, is the identification of potential errors in operator functions, tasks and requirements during test, operation and maintenance. Human Factors Analysis is presented in this Guide as a separate analysis, in order to define it adequately. However, its main applications are in conjunction with the other analyses described in this Guide where the effects of human error must be determined.

b. The data required for this analysis includes that required for the other analyses and a knowledge of human factors (listed below) that could lead to errors. Consideration of these factors should be an inherent part of Functional Hazard Analysis, Fault Hazard Analysis, and Procedure Analysis.

(1) Inherent task difficulty can be measured to a satisfactory degree through accepted laboratory and simulation techniques, whereby task failure rate under prescribed conditions can be determined.

(2) Environmental stress factors include heat, cold, darkness, noise, acceleration forces including zero gravity, vibration, extreme fatigue, or prolonged isolation. Simulation techniques have been helpful in measuring the effects of the physical environment. In analyzing fatigue and prolonged isolation, it is possible to use rational judgement of these factors' effect on humans in a given context.

(3) Design features inducing human error are those "booby traps" such as similar control knobs, located close together, for different functions. Some can be eliminated by examination, however, other more subtle examples must be analyzed. Secondary and sequential failures that can be traced to human errors due to the absence of good human engineering practices is an example of this.

(4) Task associated with "look alike" items such as installation of electrical connectors, pneumatic or hydraulic fittings are major contributors to human errors.

(5) Accessibility/vulnerability concerns the accessibility for human-induced "accidents" coupled with the vulnerability to abuse. Access to sensitive equipment and areas must be provided only to certified or qualified personnel.

(6) Level of personnel skill (relative to a specific context). This analysis evaluates the training, related experience, opportunities for practice and learning conditions of the individuals who are likely to perform a given task.

c. Human Factors Analysis is normally performed in conjunction with the other analyses as indicated below.

2. <u>Method of Analysis</u>

a. The basic method for Human Factor Analysis is as follows:

(1) Define the system (or part) failure.

(2) Identify and list human operations performed and their relationships to system tasks and functions.

(3) Determine human errors which lead to system failures.

(4) Recommend changes to reduce probability of system failure.

b. The basic method, as applied in the performance of the progressive hazard analysis previously described, is to include the following activities.

(1) Functional Hazard Analysis

(a) Identify those mission and system functions wherein the human operators play a significant role.

(b) Identify the physical environment under which the human operator must perform these functions and the resultant hazard.

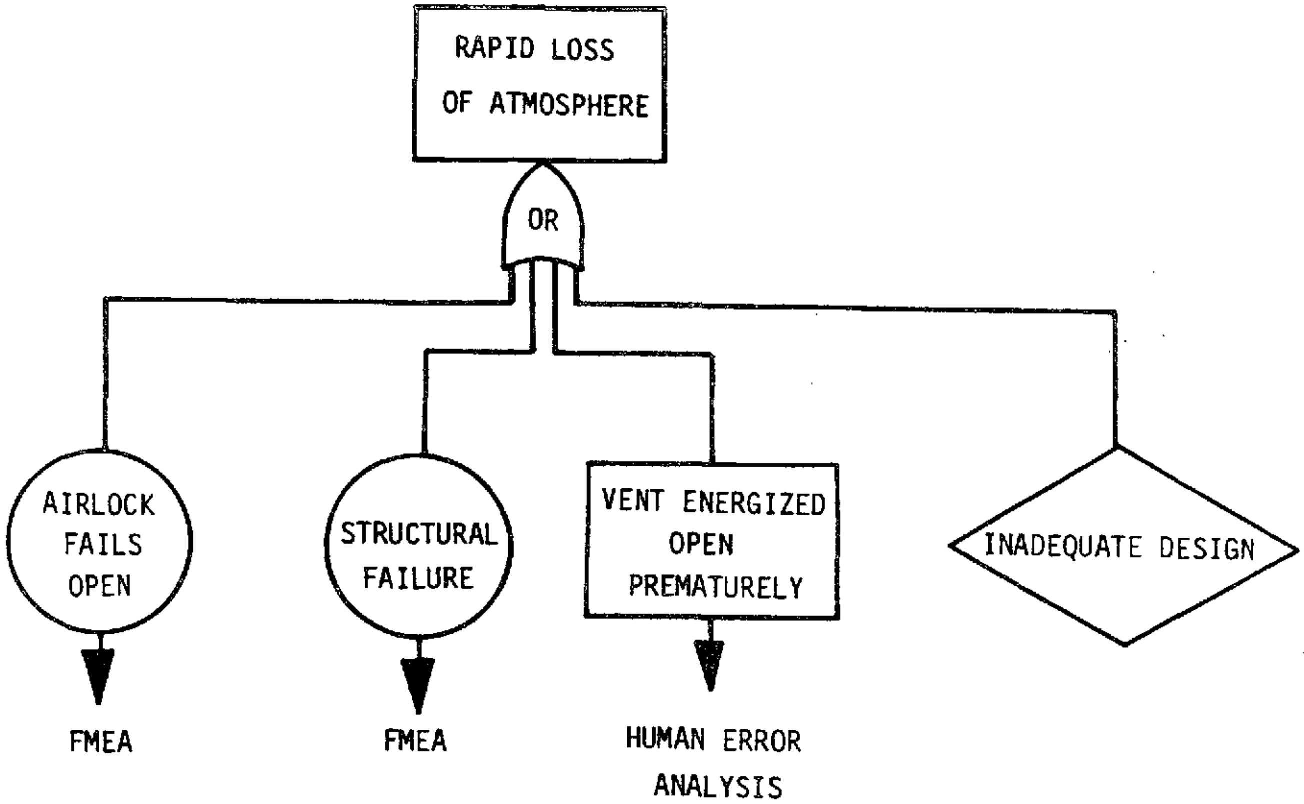
(c) Evaluate system design and training to assess its adequacy for supporting the human function.

(d) Make recommendations for improvement where inadequacies exist in requirements for design and training.

(2) Fault Hazard Analysis

(a) Identify factors which can contribute to component secondary and sequential failures. Specify those factors or hazardous events which can result from human error.

(b) Make recommendations for improvement of the system design or of specific procedures to reduce the probability of human error. See Figure 13 and supporting text for an example.



SAMPLE HUMAN FACTORS ANALYSIS

Possible Error

Crew member could press "vent open" control button out of sequence and thereby erroneously energize and open the vent valve prematurely.

Reasons for Error

The "vent open" control button looks like several other control buttons.

Recommended Corrective Action

Design an electrical or mechanical interlock which prevents premature energizing of the vent valve even if the "vent open" control button is pressed. Change appearance of look-alike control buttons so they can be readily distinguished from each other.

FIGURE 13. SAMPLE HUMAN FACTORS ANALYSIS

(c) Consider potential human operator reaction to an undesired event and to the subsystem failures which produce the undesired event. Record these potential acts in parallel with the subsystem analysis data.

(d) Examine the potential reactions so identified and determine if they may produce an error and further contribute to the hazardous situation.

(e) Evaluate the adequacy of the system design and training program and make recommendations to reduce the probability of emergency-induced human error.

(3) Procedures Analysis

(a) Identify the physical environment under which the human operator must perform the specified functions.

(b) Evaluate the human engineering aspects of the system design and the adequacy of the training program for supporting the function under the identified conditions of performance.

(c) Make recommendations for improvement where inadquacies exist in the system design and in the training program.

3. Results

Identification of human factors in operator functions, tasks and requirements during test, operation and maintenance. Recommendations for procedural, software and hardware changes to eliminate, minimize or control possible hazards due to human errors.

H. REQUIREMENTS VERIFICATION

1. The product of the analytical safety effort consists of safety visibility used in support of risk management decisions and safety requirements used to influence design or procedures that test or operate the system. It is necessary not only to establish the initial safety requirements and criteria, but to evaluate these requirements and criteria on an iterative basis to assure they accomplish the intent for which they were originated. Moreover, new requirements may be developed or existing requirements changed in order to maintain the established safety level of the system.

2. Original safety requirements and criteria stem from data extracted from experience gained on similar systems, standard system safety technology and the Functional Hazards Analysis. More detailed safety analyses such as the Fault Hazard Analysis utilizing the Logic Diagram Analysis technique will yield requirements that are unique to the evolving system.

3. Concurrently with the performance of these analyses, the original safety criteria should be assessed to verify that these requirements correctly continue to influence the design as it evolves. It is essential, as these safety requirements are developed or refined, that they be documented and that this documentation be maintained on an up-to-date basis for design use.

APPENDIX A: REFERENCES

NASA

SAFETY PROGRAM DIRECTIVE NO. 1 REVISION A	System Safety Requirements for Manned Space Flight, OMSF, Washington, D.C., December 1969.
NASA TM-X 53282	Launch Vehicle Safety Engineering for Standard Payload Module, October 20, 1965, MSFC
NASA TM-X 53612	The Systems Safety Program for a Total Space Launch Vehicle General Requirements, May 23, 1967, MSFC
NASA TM-X 53305	Standard Payload Module System Analysis Procedures for System Definition, July 26, 1965, MSFC.
NASA TM-X 53664	Systems Safety Criteria for Use In Preparation or Review of Procedures, October 17, 1967, MSFC
NASA TM-X53563	System Safety Handbook, January 6, 1967, MSFC
NASA TM-X 53388	Saturn V System Safety Program Adequacy Evaluation, February 1, 1966, MSFC
NHB 1700.1 (V 1)	NASA Safety Manual, Basic Safety Requirements, NASA Safety Office, Code DY, Washington, D.C. July, 1969.
NHB 1700.1 (V 3)	NASA Safety Manual, System Safety, NASA Safety Office, Code DY, Washington, D.C., March 1970.
NHB 5300.4 (1A)	Reliability Program Provisions for Space System Contractors, R&QA, Code KR, Washington, D.C. April 1970.
NHB 5300.4 (1D)	Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program, Washington, D.C.., December 1972.
SP 6506	An Introduction to the Assurance of Human Performance in Space Systems, R&QA, Code KR, Washington, D.C.
MSFC 85M03885	Guidelines for Performing Failure Mode, Effects and Criticality Analyses (FMECA) in the Space Shuttle

DOD

AFSC DH 1-1	Design Handbook, June 1971.
AFSC DH 1-6	Design Handbook, "System Safety", July 1971.
AFSCM 127-1	System Safety Management
AMCP 385-23	Management System Safety

MIL-STD-882	System Safety Program for Systems, and Associated Subsystems and Equipment; General Requirements for, July 1969.
AFETRM 127-1	Range Safety Manual (Volume 1), September 1972.
AFSCM 127-1	Safety, System Safety Management, Air Force Systems Command
SAMSOM 127-1	Safety, Plans, Programs and Procedures (Volume IV), System Safety Engineering, Space and Systems Organization Manual, USAF
EXHIBIT 68-8	Weapons Systems Safety Analysis Requirements, SAMSO-AFSC, Los Angeles, California, November 1968
SAMSO	System Safety Engineering, Hazard Analysis Requirements, Safety Office (SMW) SAMSO-AFSC, Los Angeles, California, July 1968 (Major P. J. Stack)
	<u>CONTRACTOR</u>
D2-113072-1	System Safety Analytical Technology - Preliminary Hazard Analysis, The Boeing Company, Revision A, December 1969.
D2-11072-2	System Safety Analytical Technology - Fault Tree Analysis, The Boeing Company, February 1970.
D2-113072-3	System Safety Analytical Technology - Fault Hazard Analysis, The Boeing Company, March 1972.
Safety Engineering Bulletin No. 3	System Safety Analytical Techniques, Electronic Industries Association, May 1971.

APPROVAL

A GUIDE FOR PERFORMING SYSTEM SAFETY ANALYSIS

By

J. M. Brush, R. W. Dpuglass III, F. R. Williamson
(Martin C. Dorman, Editor)

The information in this report has been reviewed for security classification. Review of any information concerning Department of Defense or Atomic Energy Commission programs has been made by the MSFC Security Classification Officer. This report, in its entirety, has been determined to be unclassified.

This document has also been reviewed and approved for technical accuracy.

Frederick Wrenn(?)

for L. G. Richard
Director, S&E System/Products Office